WHAT IS CLAIMED IS:

1. A system for administering electronic markets which include encrypted electronic content, the system comprising

a connection system to permit connection to a communication network having an electronic server system configured to permit communication among a community of users and for hosting of the electronic markets;

a distributed administration system, wherein any user of the community of users can be provided with a capability of configuring and administering individual ones of the electronic markets;

a set of access permissions which control access to the electronic markets, wherein the access permissions control which users of the community of users have access to the electronic markets; and

a set of usage permissions which control usage of content of the electronic markets.

2. The system according to claim 1 wherein the electronic markets have a mixture of at least one of individual users or groups.

3. The system according to claim 2 wherein the individual users and groups have different usage permissions.

4. The system according to claim 1 wherein each product has at least one user group with permission to manage properties of the product, including a capability to change the associated usage permissions or change the markets within which the product appears.

5. The system according to claim 1 wherein the content includes encrypted electronic document files.

6. The system according to claim 1 wherein the content is stored at a location separate from the access permissions and the usage permissions.

7. The system according to claim 5 wherein selections of certain ones of the access permissions and the usage permissions cause an associated market to be a private market.

8. The system according to claim 1 wherein content in the electronic markets have embedded a server location that identifies the server of the electronic server system where the access and the usage permissions are served, and a content identifier that uniquely identifies the content on the identified server.

9. The system according to claim 1 wherein access to decryption keys used to decrypt the content is controlled through at least one authenticated account on the identified permissions server.

10. The system according to claim 1 further including a paper interface to the electronic market.

11. The system according to claim 10 wherein the paper interface makes use of enhanced barcodes.

12. The system according to claim 10 wherein the paper interface permits at least one of an addition of content to an electronic market, creation of a new electronic market, altering permissions of an electronic market, and obtaining content from the electronic market.

13. A method for administering electronic markets which include electronic products, the method comprising:

providing connection to a communication network having at least one server which permits communication among a community of users;

hosting at least one electronic market on the at least one server;

distributing administration of the electronic markets, wherein each user of the community of users can be provided with a capability of administering individual ones of the electronic markets;

providing a set of access permissions;

controlling access to the electronic markets by use of the access permissions;

providing a set of usage permissions; and

controlling usage of products of the electronic markets by the usage permissions.

14. The method according to claim 13 wherein the content is electronic document files.

15. The method according to claim 13 wherein the content is stored at a location separate from the access permissions and the usage permissions.

16. The method according to claim 15 wherein selections of certain ones of the access permissions and the usage permissions cause an associated market to be a private market.

17. The method according to claim 13 further including a paper interface to the electronic market.

18. The method according to claim 17 wherein the paper interface permits at least one of, addition of content to an electronic market, creation of a new electronic market, altering permissions of an electronic market, and obtaining content from the electronic market.

19. A method of creating and administrating an electronic marketplace comprising:

forming a network of a community of users electronically interconnected via an electronic communication system, the community of users being a subset of users having access to the electronic communication system;

logging on, by a first user, to the network of the community of users;

creating, by the first user, an electronic market;

specifying access permissions to the market for at least one of other users or groups of the community of users;

uploading electronic content to the market;

creating a unique content identifier identifying the uploaded content;

storing the content identifier on the server;

specifying usage permissions to be associated for the uploaded content;

embedding into the content the content identifier of the product and location of a server where the access and usage permissions have been stored; and

encrypting the content.

20. The method of claim 19 further comprising having a second user or a group log onto a server of the network of community of users;

accessing, by the second user or group the electronic market created by the first user;

checking to determine access permissions for the second user or group for access to the market;

determining access permissions for at least one of the second user and group exists;

checking for at least one of the second user and the group for access permissions for all content existing in the electronic market;

displaying content representations for all content determined to have access permission for at least one of the second user and group;

selecting by the second user or group at least one of the content representations;

checking to determine whether the second user or group has additional access permissions for the selected content;

checking whether the second user or group has usage permissions for the selected content;

determining the second user or group has access permissions for the selected content;

checking whether the second user or group has usage permissions for the selected content;

determining the second user or group has the usage permissions for the selected content;

displaying the usage permissions and fees associated with the selected content to the second user or group.

21. The method of claim 20 further comprising:

generating a license by encrypting the content key with a user key and attaching a verification key;

downloading by the second user or group the content and the license;

selecting the encrypted file, by the second user or group, and invoking operation of a client operating system;

checking to determine whether a license does exist;

generating, when it is determined a license exists, the content key by decrypting a license with the user key;

decrypting content of the content key;

checking the content with the verification key;

invoking interpretation operations;

disabling save-as and/or print commands which would permit the second user or group to alter the content; and

rendering the content to the second user or group in a readable format.

22. The method according to claim 19 wherein the content is provided via at least one of an encrypted e-mail message, from a server of the system of community of users, or on a CD ROM.

23. The method of claim 19 wherein the step of checking if a license exists determines no license exists further including,

determining the server location and content identifier to exist with the encrypted content;

downloading the license for the specified encrypted content;

again clicking on the encrypted content;

determining a license exists;

generating content key by decrypting the license with the user key;

decrypt the content with the content key;

check the content with the verification key;

invoke the content viewer;

disable determined commands of the viewer; and

rendering the content to at least one of the second user or group.

24. A system for controlling usage of content comprising:

encrypted content that has embedded at least one usage permissions server identifier and at least one encrypted content identifier;

a reader on a computer that reads the at least one usage permissions server identifier and the at least one encrypted content identifier;

a communication system that communicates the at least one encrypted content identifier to at least one identified usage permissions server;

a permissions server that receives the at least one encrypted content identifier, and that permits usage of the at least one encrypted content identified by the at least one encrypted content identifier, based on usage

permissions associated with the identified content and at least one identified authenticated account associated with the identified permissions server by communicating an electronic key to the computer that communicated to the permissions server; and

a viewer or player that displays or plays the identified encrypted content after using the communicated electronic key to decrypt the identified encrypted content.

25. The system according to claim 24 wherein access permissions associated with administering usage permissions for encrypted content can be associated with multiple accounts on the permissions server.

26. The system according to claim 25 wherein the permissions server identifier is a URL and administration of usage permissions can be done using a web browser that has access to the permissions server through the web.

27. The system according to claim 26 wherein permissions are managed using a permissions matrix.

28. The system according to claim 24 wherein permissions for encrypted content are associated with accounts using an object database.

29. The system according to claim 24 wherein the encrypted content is electronic documents.

30. The system according to claim 24 wherein the encrypted content identifiers are non-location-based URLs.

31. The system according to claim 25 wherein access permissions include permission to change the locations of electronic content.

32. The system according to claim 24 wherein a copy of the encrypted content is stored on the same server as the permissions matrices.